UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	
-against-	:	Notice of Motion to Suppress
	:	
ALEXEY GAVINO,	:	
	:	22-CR-136 (RPK)
Defendant.	:	

PLEASE TAKE NOTICE, that the defendant, **Alexey Gavino**, by his attorney **Marissa Sherman**, of the Federal Defenders of New York, and upon the accompanying memorandum of law, will move the Court, before the Honorable Judge Rachel P. Kovner, United States District Judge for the Eastern District of New York for an Order:

1. Suppressing all evidence recovered as a result of the unconstitutional search of Mr. Gavino's iPhone 11 and all evidence recovered as a fruit of the unconstitutional search, pursuant to Fed. R. Crim. P. 12(b)(3)(C) and the Fourth and Fifth Amendments of the United States Constitution, and

2. In the alternative, directing that a hearing be held outside the presence of the jury before trial as to the admissibility of the evidence; and,

3. Granting such other and further relief as the Court may deem just and proper.

DATED: BROOKLYN, N.Y.
December 1, 2022

Marissa Sherman

Marissa Sherman
Attorney for Alexey Gavino
Federal Defenders of New York, Inc.
One Pierrepont Plaza, 16th Floor
Brooklyn, NY 11201
(347) 802-7048
Marissa_Sherman@fd.org

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	
-against-	:	MEMORANDUM OF LAW
	:	
ALEXEY GAVINO,	:	22-CR-136 (RPK)
	:	
Defendant.	:	

Memorandum of Law
in Support of
Motion to Suppress Evidence

Marissa Sherman
Marissa Sherman
Attorney for Alexey Gavino
Federal Defenders of New York, Inc.
One Pierrepont Plaza, 16th Floor
Brooklyn, NY 11201
(347) 802-7048
Marissa_Sherman@fd.org

PRELIMINARY STATEMENT

Alexey Rene Gavino, through counsel, moves this Court to suppress all evidence obtained as a result of the unconstitutional manual search of Mr. Gavino's iPhone 11. Mr. Gavino's iPhone was allegedly seized pursuant to the border search doctrine when Mr. Gavino was returning to the United States following a trip to the Dominican Republic. First, suppression is required because law enforcement forced Mr. Gavino to decrypt his iPhone by providing his passcode, in violation of the Fifth Amendment and *Miranda v. Arizona*, 384 U.S. 436 (1966). Second, suppression is required because in light of *Riley v. California*, 573 U.S. 373 (2014)—and its recognition that an individual's privacy interest is at its peak with regard to digital device searches—the Fourth Amendment required a warrant, or at the very least, be supported by reasonable suspicion or probable cause.

STATEMENT OF FACTS[1]

On August 30, 2021, Alexey Gavino arrived at John F. Kennedy International Airport ("JFK") in Queens, New York aboard a JetBlue flight from the Dominican Republic. *See* Exhibit A, *Christie Affidavit*, ¶ 7. Officers from United States Customs and Border Patrol ("CBP") referred him for an enforcement examination, and then directed Mr. Gavino to a secondary inspection. *Id.* at ¶ 8. The secondary inspection occurred in a closed room. *See* Exhibit B, *Gavino Declaration*.

As part of the secondary inspection, the CBP officers searched Mr. Gavino's person. *See* Exhibit A, *Christie Affidavit*, ¶ 8. The officers found Mr. Gavino's iPhone 11 on his person and seized the device. *Id*. The phone was out of batteries and the CBP officers plugged the phone into a charger. *See* Exhibit B, *Gavino Declaration*. When the phone was charged enough to turn on, the officers directed Mr. Gavino to provide his passcode. *Id*; *see also* Exhibit A, *Christie Affidavit*, ¶ 8. Mr. Gavino initially did not do as the officers commanded and asked what would happen if he did not provide his passcode. *See* Exhibit B, *Gavino Declaration*. The officers instructed Mr. Gavino that they would confiscate his phone if he did not comply with their directive. *Id.* Based upon that instruction, Mr. Gavino complied with the officers' commands. Significantly, at the time during which Mr. Gavino was compelled to unlock his device, he had not been advised of his *Miranda* rights. *Id.*

The agents proceeded to conduct a manual search of Mr. Gavino's phone. A manual search is a search by which law enforcement opens a device and views its contents in a way that any lay person might be capable of doing.[2] For instance, law enforcement may click through various

[1] Information provided in the "Statement of Facts" is based on discovery provided by the government, a review of court records and documents, and defense counsel's own investigation.

[2] *See Abidor v. Napolitano*, 990 F. Supp. 2d 260, 269–70 (E.D.N.Y. 2013) ("A quick look entails only a cursory search that an officer might be capable of doing simply by clicking through various folders.).

applications to view photos, emails, call logs, etc.[3] While manually searching Mr. Gavino's phone, the officers purportedly found images and videos depicting child pornography. *See* Exhibit A, *Christie Affidavit*, ¶ 9. The CBP officers then contacted Homeland Security Investigations (hereinafter "HSI") agent Shannon Christie. *Id.* at ¶ 10. Agent Christie conducted a further search of the device and purportedly found seven videos showing child pornography in the WhatsApp application. *Id.*

HSI Agent Shannon Christie later secured a warrant to conduct a forensic search of Mr. Gavino's cell phone. In the warrant affidavit, the agent included and cited the facts regarding what was found in the manual search of the phone as a basis for probable cause to search the phone forensically. *See* Exhibit A, *Christie Affidavit*, ¶ 6-10.

[3] *Id.* (citing cases which detail the features of a manual search).

ARGUMENT

The manual search of Mr. Gavino's iPhone violated the Fifth and Fourth Amendments. *See* U.S. CONST. amends. V and IV. With respect to the Fifth Amendment violation, the requirement that Mr. Gavino unlock and decrypt his cell phone was compulsive, testimonial, and self-incriminating. Mr. Gavino was also forced to provide his passcode without first being advised of his *Miranda* rights. Under the Fourth Amendment, a warrant was required for the manual search, or at the very least, the search should have been supported by reasonable suspicion or probable cause. Accordingly, all evidence obtained from the manual search must be suppressed. Because the evidence obtained from the forensic search of Mr. Gavino's cell phone is the fruit of the initial search, the forensic search evidence must also be suppressed. *See, e.g., United States v. Djibo*, 151 F. Supp. 3d 297, 309 (E.D.N.Y. 2015) (suppressing evidence obtained from warrant-supported forensic search of digital device at the border as the fruit of prior Fifth and Fourth Amendment violative search).

I. The compelled decryption of Mr. Gavino's cell phone violated the Fifth Amendment.

The Fifth Amendment to the United States Constitution provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The Fifth Amendment applies when the government seeks to (1) *compel* an individual to provide (2) a *testimonial* communication or act that is (3) *incriminating*. *See Fisher v. United States*, 425 U.S. 391, 409 (1976).

With respect to the first prong, law enforcement agents compelled Mr. Gavino to provide them with his numeric key. And with regard to the third prong, it is clear that law enforcement's access to Mr. Gavino's phone yielded incriminating evidence. *See* Exhibit A, *Christie Affidavit*, ¶ 9-10.

The critical inquiry therefore is the second prong: whether providing the numeric key was a "testimonial" act under the Fifth Amendment. *See, e.g.*, *United States v. Warrant*, No. 19-mj-71283-VKD-1, 2019 WL 4047615, at *1 (N.D. Cal. Aug. 26, 2019) ("For purposes of this application, the critical issue is whether compulsory application of a biometric feature is a testimonial communication."); *In re Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019) ("[T]he issue is whether the use of a suspect's biometric feature to potentially unlock an electronic device is testimonial under the Fifth Amendment."); *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1342 (11th Cir. 2012) ("What is at issue is whether the *act of production* may have some testimonial quality sufficient to trigger Fifth Amendment protection . . . . Thus, we focus on whether Doe's act of decryption and production would have been testimonial.").

A. Providing a numeric passcode is "testimonial."

As a threshold matter, requiring Mr. Gavino to provide his device's passcode or password is testimonial under the "act of production" doctrine. Under the Supreme Court's most recent formulation, an act of production can be testimonial where it "may implicitly communicate" facts such as an admission that certain documents exist, were in an individual's custody, and were authentic. *United States v. Hubbell*, 530 U.S. 27, 36 (2000) (citation omitted). That the act of production requires an individual to reveal "the contents of his mind" is strong evidence of a "testimonial aspect." *Id.* at 43.

Applying this framework, many federal and state courts have found that compelling an individual to provide their passcode is testimonial under the Fifth Amendment, as it forces him to "reveal the contents of his own mind." *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (compelled "decryption and production of the

contents" of hard drives "would be testimonial" because it would "require the use of the contents" of defendant's mind and reveal "whether any files exist and are located on the hard drives"); *see also United States v. Apple MacPro Computer*, 851 F.3d 238, 247–58 (3d Cir. 2017) (applying the Eleventh Circuit's reasoning in *In re Grand Jury Subpoena* but finding that the foregone conclusion doctrine compelled a different result on the facts); *United States v. Jimenez*, 419 F. Supp. 3d 232, 233 (D. Mass. 2020) ("Whether the defendant is forced to reveal his passcode or unlock the phone in the presence of law enforcement does not impact the analysis; both situations would force defendant to 'disclose the contents of his own mind' and accordingly are testimonial acts violating the Fifth Amendment."); *United States v. Warrant*, No. 19-mj-71283-VKD-1, 2019 WL 4047615, at *2 (N.D. Cal. Aug. 26, 2019) (noting that prosecution "acknowledges . . . a consensus has emerged that a suspect may not be compelled to divulge his or her password to law enforcement" since it would "require disclosure of the contents of the suspect's mind"); *SEC v. Huang*, No. 15-269, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) (compelled production of smartphone passcodes is testimonial); *Seo v. State*, 148 N.E. 3d 952, 955 (Ind. 2020) (compelled production of an unlocked smartphone is testimonial because it conveys suspect's knowledge of password as well as possession and existence of files on device).

B. The command that Mr. Gavino provide his iPhone passcode, especially in the absence of *Miranda*, requires suppression.

Mr. Gavino's acts—unlocking and decrypting his iPhone by providing its numeric key—were compelled, incriminatory, and testimonial, and as a result, the manual search of his phone violated the Fifth Amendment. Additionally, because Mr. Gavino had not been *Mirandized* at the time he was asked to unlock his device, the manual search further violated the Fifth Amendment. An Eastern District of New York case, *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), is particularly instructive on this point.

In *Djibo*, the defendant was being investigated for heroin trafficking when law enforcement received intelligence that he would be traveling by air from the United States to London. *Id.* at 298–99. Law enforcement agents targeted Mr. Djibo for a "border search" and seized, *inter alia*, his iPhone 5. *Id.* at 299. The agents then asked Mr. Djibo for his passcode, which he provided. *Id.* The agents purported to do a "basic" search of the phone at that time to look for evidence of currency or other illegal activity. *Id.* at 302. A month later, the agents obtained a search warrant to conduct a forensic search. *Id.* The court held that the statement identifying the passcode to Mr. Djibo's iPhone was suppressible under the Fifth Amendment, *id.* at 306, and that evidence from the subsequent, warrant-supported forensic search was suppressible as its fruit, *id.* at 310.

Just as in *Djibo*, Mr. Gavino's passcode was taken from him in violation of *Miranda*, making the subsequent manual and forensic searches of his phone suppressible as its fruit. For this additional reason, all evidence found as a result of the manual search must be suppressed.

II. The Fourth Amendment required a warrant for the manual search of Mr. Gavino's device.

After stopping Mr. Gavino and referring him to secondary inspection, customs officers searched him and recovered an iPhone. They not only confiscated Mr. Gavino's iPhone but proceeded to conduct a manual search on the device without a warrant. The manual search of Mr. Gavino's phone violated the Fourth Amendment by infringing upon the expansive privacy interests inherent within his digital device.

A. *Riley v. California* established that an individual's privacy interest is at its peak with regard to digital device searches.

In *Riley v. California*, 573 U.S. 373 (2014), the Supreme Court *unanimously* held that law enforcement must obtain a warrant to search digital information on cell phones that are seized during a lawful arrest. In reaching this conclusion, the Court did not distinguish between "manual

searches" as defined above (at 2), and "forensic searches."[4] The Court employed the traditional Fourth Amendment balancing test "by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Riley*, 573 U.S. at 385. And the Court quite dramatically emphasized the significant privacy interests inherent in a cellular device. The Court observed that cell phones "hold for many Americans the privacies of life[,]" *id.* at 403, and that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house[,]" *id.* at 396.

The Court's privacy analysis took into account both the quantitative and the qualitative differences between a cell phone and other objects that might be subjected to a search. *Id.* at 393–95. Quantitatively, the Court explained, cell phones are different because they "are in fact minicomputers" and have an "immense storage capacity." *Id.* at 393. The average smartphone in 2014 had the ability to hold "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394. Moreover, cell phones can hold several different *types* of information such as "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." *Id.*

All of this led the Court to conclude that a cell phone's quantitative storage capacity has four consequences for privacy. *Id.* First, because it "collects in one place many distinct types of information," cell phones are much more revealing than any isolated record. *Id.* Second, even just considering each individual type of information, like photographs for example, a cell phone's storage capacity allows just that one type of information to "convey far more than previously

[4] Forensic searches are searches that occur when agents use forensic software to copy the entire contents of a device, including data that users have deleted or may be unaware of, and conduct a comprehensive search based on that copy. *See United States v. Cotterman*, 709 F.3d 952, 962–63 & n.9 (9th Cir. 2013).

possible." *Id.* ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."). Third, the information routinely preserved on cell phones dates back much further than information carried around physically. *Id.* at 394–95. And fourth, cell phones are so pervasive—owned by 90 percent of American adults—that they will almost always be present for police to scrutinize in a way that physical records are not. *Id.* at 395.

Qualitatively, cell phones are different from other items subject to searches in that they are highly personal and reveal information such as where people have been or the nature of their private interests or concerns. *Id.* at 395–96. Cell phones provide detailed information about a person's life such as political affiliation, addictions, budget, hobbies, and romantic life. *Id.* at 396. Furthermore, cell phones are not self-contained but instead can be used to access data located on remote servers such as the Cloud. *Id.* at 397.

This analysis by the *unanimous* Supreme Court in *Riley* established, in effect, that an individual's privacy interest is at its peak with regard to searches of digital devices. *See id.* at 385 (noting that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."); *id.* at 396–97 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."). Given the strength of this recognition, these principles should apply with equal force to other Fourth Amendment contexts outside of searches incident to arrest.

B. The Fourth Amendment weighing of interests in the border search context requires a warrant, in light of *Riley*.

The Supreme Court has repeatedly emphasized "that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967). Similar to the "search incident to a lawful arrest" exception, the border search exception has been a "longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained[.]" *United States v. Ramsey*, 431 U.S. 606, 621 (1977). This exception is rooted in the "right of the sovereign to protect itself by stopping and examining persons and property crossing into this country[.]" *Id.* at 616. Therefore, under the Fourth Amendment, such searches have been deemed "reasonable simply by virtue of the fact that they occur at the border[.]" *Id.*

Although "Congress has granted the Executive plenary authority to conduct *routine* searches[5] and seizures at the border, without probable cause or a warrant," *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985) (emphasis added), the Supreme Court has utilized a balancing test to determine whether *nonroutine* border searches are reasonable under the Fourth Amendment. *See, e.g., id.* at 538 ("[T]he Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior."); *United States v. Flores-Montano*, 541 U.S. 149, 152–56 (2004) (balancing the government's interest in preventing the entry of unwanted persons and effects against the individual's privacy and property interests in his fuel tank). Under this reasonableness test, the permissibility of a particular border search "is judged

[5] "Routine" searches have a limited intrusion upon an individual's privacy and consist of "limited searches for contraband or weapons through a pat-down; the removal of outer garments such as jackets, hats, or shoes, the emptying of pockets, wallets, or purses; the use of a drug-sniffing dog; the examination of outbound materials; and the inspection of luggage." Yule Kim, *Protecting the U.S. Perimeter: Border Searches Under the Fourth Amendment*, Congressional Research Service Report for Congress No. RL31826 at 9 (June 29, 2009) (collecting circuit cases).

by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests." *Montoya de Hernandez*, 473 U.S. at 537 (internal quotation marks and citations omitted). In conducting this balancing test, the Court has advised that "[t]he government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

Prior to the Supreme Court's decision in *Riley*, a number of courts held that forensic border searches of digital devices were nonroutine and required, at least, reasonable suspicion. *See, e.g.*, *United States v. Laich*, No. 08-20089, 2010 WL 259041, at *4 (E.D. Mich. 2010) (holding that probable cause was needed for the government to permanently seize a laptop and forensically search it); *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (concluding that reasonable suspicion was required for a forensic search of a laptop); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 548 (D. Md. 2013) ("[A] forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulable suspicion."). Prior to *Riley*, courts also held that manual border searches were routine, thereby requiring no level of suspicion. *See, e.g.*, *United States v. Linarez-Delgado*, 259 F. App'x 506, 509 (3d Cir. 2007) (unpublished) (holding that no suspicion was required for border search of camcorder); *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008) ("[W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.").

However, in light of the Court's *unanimous* recognition in *Riley* that all searches of cell phones—both manual and forensic—impose the highest infringement upon an individual's

privacy, all searches of digital content at the border should be considered non-routine and thus require a probable cause warrant.[6]

C. The warrantless, manual search of Mr. Gavino's iPhone violated the Fourth Amendment.

Because the manual search of Mr. Gavino's iPhone was conducted without a warrant, all evidence found as a result must be suppressed. *See, e.g.*, *Djibo*, 151 F. Supp. 3d at 309 (suppressing evidence obtained from warrant-supported forensic search of digital device at the border as the fruit of prior Fifth and Fourth Amendment violative search).

III. Alternatively, the Fourth Amendment requires that the manual search of Mr. Gavino's iPhone be supported by reasonable suspicion or probable cause.

Even if this Court were to disagree that all manual searches of digital devices at the border require a warrant, this Court should still hold that, given the privacy interests at stake, a manual search of a cell phone at the border must be supported by reasonable suspicion or probable cause that evidence of a crime would be found in the cell phone.

A number of post-*Riley* courts that have addressed the issue of the level of suspicion required for *forensic* searches of digital devices at the border have held that the Fourth Amendment balancing weighs in favor of some level of particularized suspicion. *See, e.g.*, *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018) ("[I]n light of the Supreme Court's decision in *Riley*, a forensic search of a phone must be treated as nonroutine, permissible only on a showing of individualized suspicion."); *United States v. Cano*, 934 F.3d 1002, 1007 (9th Cir. 2019) ("[W]e conclude that . . . *forensic* cell phone searches require reasonable suspicion."). Mr. Gavino respectfully submits that just as the *Riley* court made no distinction in the Fourth Amendment

[6] This is an open question in the Second Circuit in light of *Riley*. However, some courts that are non-binding upon this Court have disagreed with this position. *See, e.g, Alasaad v. Mayorkas*, --- F.3d ---, 2021 WL 521570 at *1 (1st Cir. Feb. 9, 2021) (holding that manual searches of digital devices are routine and may be conducted without reasonable suspicion).

balancing between manual and forensic searches, neither should this Court. That is, since *forensic* device searches require a level of particularized suspicion, the same should hold true for *manual* searches—which themselves also implicate expansive privacy interests. And whether the standard is reasonable suspicion or probable cause, the suspicion must be that officers have reason to believe evidence of a crime would be found specifically within the digital device.

Because the law enforcement agents did not have any particularized suspicion that evidence of a crime would be found on Mr. Gavino's iPhone at the time of the manual search, the evidence found as a result of that search must be suppressed.

IV. Evidence obtained from the forensic search of Mr. Gavino's phone was the unlawful fruit of the unconstitutional manual search.

If this Court were to suppress the evidence found from the manual search of Mr. Gavino's iPhone, it should also suppress the evidence found from the forensic search that was subsequently conducted. The evidence from the forensic search constitutes the fruit of the unconstitutional manual search as it was relied upon for the search warrant and was thereby "come at by exploitation of that illegality[.]" *Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *see also, e.g., Djibo*, 151 F. Supp. 3d at 309 (suppressing evidence obtained from warrant-supported forensic search of digital device at the border as the fruit of prior Fifth and Fourth Amendment violative search); *United States v. Laynes*, 2020 WL 4901644 at *10 (S.D. Ohio August 20, 2020) (suppressing evidence from forensic cell phone search as fruit of unconstitutional manual search at the border) ("Additionally, all subsequent evidence of child pornography found on Defendant Laynes's iPhone is suppressed as the fruit of the poisonous tree."); *Murray v. United States*, 487 U.S. 533, 537 (1988) (recognizing that illegal warrantless entry would taint subsequently obtained search warrant "if the agents' decision to seek the warrant was prompted by what they had seen

during the initial entry, or if information obtained during that entry was presented to the Magistrate and affected his decision to issue the warrant.").

CONCLUSION

For all of the aforementioned reasons, the manual search of Mr. Gavino's iPhone 11 violated the Fifth and Fourth Amendments. All evidence seized from the cell phone and any fruits thereof, including evidence from the subsequent forensic search, must be suppressed. To the extent the merits of the instant motion are not readily apparent on the briefs, Mr. Gavino respectfully requests an evidentiary hearing to determine the admissibility of the evidence complained of.

Marissa Sherman

Marissa Sherman
Attorney for Alexey Gavino
Federal Defenders of New York, Inc.
One Pierrepont Plaza, 16th Floor
Brooklyn, NY 11201
(347) 802-7048
Marissa_Sherman@fd.org

cc: AUSA Benjamin Weintraub (by ECF and E-mail)
Chambers of the Hon. Rachel P. Kovner (by E-mail)

EXHIBIT A

WK:LZ

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE WIRELESS TELEPHONE, CURRENTLY LOCATED IN THE EASTERN DISTRICT OF NEW YORK	**To Be Filed Under Seal** APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICE Case No. 21 MJ 1014

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, SHANNON CHRISTIE, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), and I have been employed by HSI since 2019. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have received training and participated in investigations regarding, among other things, unlawful drug trafficking, and have used a variety of investigative techniques, including, but not limited to, interviews of witnesses, interviews of suspects, physical surveillance and review and analysis of phone records. I have participated in multiple investigations with HSI and have participated in the execution of search warrants involving electronic evidence of the type requested here.

3. This affidavit is based on my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement personnel, and my training, experience, and advice received concerning the use of electronic devices in criminal activity and the forensic analysis of electronically stored information ("ESI"). This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is the following device (the "DEVICE"): A red iPhone 11, which can be identified by its assigned call number: 917-573-8920; and by its IMEI number: 352900111298084. This DEVICE is currently in my possession within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. As described in more detail below, on August 30, 2021, Alexey Rene Gavino was stopped at John F. Kennedy International Airport ("JFK") in possession of videos of young children engaged in sexually explicit acts with adults. Based on the below, there is probable cause to believe Gavino violated Title 18, United States Code, Sections 2252 and 2252A (possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children), and Title 21, United States Code, Sections 841 (possession of a controlled substance with intent to distribute) (the "Subject Crimes") and that there is evidence of the Subject Crimes on the DEVICE. Through my own

investigation and discussions with other law enforcement agents, I have learned the following facts.

7. On or about August 30, 2021, Gavino arrived at John F. Kennedy International Airport ("JFK") in Queens, New York aboard a JetBlue flight from the Dominican Republic.

8. During a previous trip approximately two years ago, Gavino had been found carrying approximately $40,000 in undeclared currency. Accordingly, as Gavino passed through Immigration and Customs on August 30, 2021, officers from United States Customs and Border Patrol ("CBP") referred him for an enforcement examination, and Gavino was directed to secondary inspection. A CBP officer conducted a border search of Gavino's person and found the DEVICE. A CBP officer asked Gavino to provide the passcode for the DEVICE, and Gavino complied. A CBP officer entered the passcode into the DEVICE and conducted a superficial search of the DEVICE.

9. The CBP officer searching the DEVICE saw images and videos depicting child pornography. Accordingly, the DEVICE was seized.

10. CBP then called HSI, and I responded. I conducted a superficial search of the DEVICE in the presence of CBP officers, and found seven videos showing child pornography in the WhatsApp application on the DEVICE. These included videos depicting prepubescent girls performing oral sex on individuals who appeared to be adult men. One video showed a prepubescent girl, unclothed, engaging in sexual intercourse with an individual who appeared to be an adult man. I also saw a video that, based on its location in the recent photos folder on the DEVICE, appeared to have been made by Gavino, showing a large amount of

marijuana. Finally, I saw photographs that, based on their location in the recent photos folder on the DEVICE, appeared to have been taken by Gavino, showing large stacks of cash.

11. I then interviewed Gavino in the presence of other law enforcement officers. I gave Gavino a *Miranda* warning, and he waived his *Miranda* rights both orally and in writing. Gavino admitted that: (a) he had approximately twenty videos and images of child pornography saved on the DEVICE; (b) he used the DEVICE to participate in a group on the Telegram app in which he discussed child pornography with other group members; and (c) the DEVICE included records reflecting his purchase of child pornography. He further disclosed that he had received child pornography on the DEVICE from an individual saved as a contact on the DEVICE and designated as "CP." I looked at the contact "CP" and saw that it was associated with the phone number (973) 348-3367.

12. Based on my training and experience, the amount of marijuana depicted in the video on the DEVICE is consistent with distribution, not with personal use. Also based on my training and experience, large stacks of cash often represent the proceeds of sales of illicit goods, such as narcotics.

13. Based on the fact that images and videos depicting prepubescent children engaged in sexual acts were found on the DEVICE; that Gavino admitted to purchasing child pornography and receiving it onto the DEVICE; that Gavino acknowledged using the DEVICE to communicate with other individuals about child pornography via a group messaging application; and that a video and images of a large amount of marijuana and stacks of cash were found on the DEVICE; there is probable cause to believe that there is additional evidence of the Subject Crimes on the DEVICE.

14. The DEVICE is currently in the lawful possession of HSI. It came into HSI's possession when it was seized following the border search, as set forth in detail above. Therefore, while HSI might already have all necessary authority to examine the DEVICE, I seek this additional warrant out of an abundance of caution to be certain that a forensic examination of the DEVICE will comply with the Fourth Amendment and other applicable laws.

15. The DEVICE is currently in my possession within the Eastern District of New York. In my training and experience, I know that it has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of HSI.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video;

storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

17. Based on my training, experience, and research, I know that the DEVICE has capabilities that allow it to serve as a wireless telephone. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. Photos, videos, and other records that have been stored on a wireless mobile Apple device, such as an iPhone, may be backed up and stored on iCloud, Apple's cloud storage and cloud computing service, and associated with the iPhone user's iCloud account. Such photos, videos, and other records may be stored on iCloud even after they are removed from an iPhone.

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

24. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation relating to a criminal organization. Based upon my training and experience, I have learned that online criminals actively search for criminal

affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Shannon Christie

Shannon Christie
Special Agent
Department of Homeland Security, Homeland Security Investigations

Subscribed and sworn to before me by telephone
on August 31, 2021

Marcia M. Henry

HON. MARCIA M. HENRY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is the following device (the "Device"): A red iPhone 11, which can be identified by its assigned call number: 917-573-8920; and by its IMEI number: 352900111298084. This device is currently in my possession within the Eastern District of New York.

.

.

ATTACHMENT B

1. All information or records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 2252 and 2252A (possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children), and Title 21, United States Code, Sections 841 (possession of a controlled substance with intent to distribute) (altogether, the "Subject Crimes") and involve Alexey Rene Gavino, including:

a. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

b. Motion pictures, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

c. Correspondence and records pertaining to violation of the Subject Crimes including, but not limited to, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

d. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;

e. Communications with any minor related to the transfer of obscene material or to any sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

f. Any child pornography as defined by 18 U.S.C. § 2256(8);

g. Any visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

h. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, electronic mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

i. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

j. All communications with the contact in the Device's contact list designated as "CP" with the phone number (973) 348-3367;

k. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the Subject Crimes, including, but not limited to, sales receipts, warranties, bills for Internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts and photographs;

l. Lists of co-conspirators and related identifying information;

m. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

n. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

o. any information recording Gavino's schedule or travel from July 1, 2021 to the present;

p. all bank records, checks, credit card bills, account information, and other financial records; and

q. Email address(s) and other identifiers associated with Gavino's iCloud account and iCloud settings on the Device.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* IN THE MATTER OF THE SEARCH OF ONE WIRELESS TELEPHONE, CURRENTLY LOCATED IN THE EASTERN DISTRICT OF NEW YORK	)	Case No. 21 MJ 1014

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 14, 2021 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: August 31, 2021 @ 4:08 p.m.

Marcia M. Henry
Judge's signature

City and state: Brooklyn, New York

The Honorable Marcia M. Henry U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 21 MJ 1014	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The property to be searched is the following device (the "Device"): A red iPhone 11, which can be identified by its assigned call number: 917-573-8920; and by its IMEI number: 352900111298084. This device is currently in my possession within the Eastern District of New York.

.

.

ATTACHMENT B

1. All information or records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 2252 and 2252A (possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children), and Title 21, United States Code, Sections 841 (possession of a controlled substance with intent to distribute) (altogether, the "Subject Crimes") and involve Alexey Rene Gavino, including:

a. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

b. Motion pictures, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

c. Correspondence and records pertaining to violation of the Subject Crimes including, but not limited to, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), or other obscene material;

d. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;

e. Communications with any minor related to the transfer of obscene material or to any sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

f. Any child pornography as defined by 18 U.S.C. § 2256(8);

g. Any visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);

h. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, electronic mail messages, chat logs and electronic messages, other digital data files and web cache information, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

i. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

j. All communications with the contact in the Device's contact list designated as "CP" with the phone number (973) 348-3367;

k. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the Subject Crimes, including, but not limited to, sales receipts, warranties, bills for Internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts and photographs;

l. Lists of co-conspirators and related identifying information;

m. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

n. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

o. any information recording Gavino's schedule or travel from July 1, 2021 to the present;

p. all bank records, checks, credit card bills, account information, and other financial records; and

q. Email address(s) and other identifiers associated with Gavino's iCloud account and iCloud settings on the Device.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

EXHIBIT B

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA

-against-

ALEXEY GAVINO 22-CR-136 (RPK)

DEFENDANT.
----------X

I, ALEXEY GAVINO hereby declare under the penalties of perjury, pursuant to Title 28 U.S.C. 1746, that the following is true and correct:

1. I am the defendant in the above-captioned case[1].
2. My lawyer prepared this declaration.
3. On August 30, 2021, I arrived at John F. Kennedy Airport on a flight from the Dominican Republic.
4. As I was in the line to go through customs, officers from Customs and Border Patrol told me to leave the line and directed me to a room.
5. There were three officers from Customs and Border Patrol in the room with me. I believed if I tried to leave the room, the officers would stop me.
6. While I was in the room, the officers started going through all of my luggage.
7. The officers also searched my person.
8. My iPhone 11 was on my person, and the officers took my iPhone from my person.
9. My iPhone 11 was out of batteries, and the officers plugged my phone into a charger.
10. The officers then asked for the passcode to my phone.
11. I did not immediately give my passcode and asked what would happen if I did not give my passcode. The officers told me that if I did not give my passcode, they would not give my phone back.

[1] Because this declaration is being submitted for the limited purpose of establishing that the search of my phone was unconstitutional, I have not set forth each and every fact and or detail of the circumstances surrounding the search and seizure of my phone and prior encounters with law enforcement.

12. I did not believe I had the right to refuse to give the officers my passcode.
13. The officers directed me to write down my passcode, and I complied with their directive.
14. After I gave the officers my passcode, one of the officers directed me to another room, and sat with me in the other room.
15. The officers from Customs and Border Patrol did not read me my *Miranda* rights before asking me for my passcode or going through my phone.

Dated: 12/01/22

s/
signed by Marissa Sherman on behalf of Alexey Gavino with prior client authorization